Windows 2000 Networking & Communications Features

Peter S. Ford
Network Architect
Windows Networking & Communications
Microsoft Corporation

Objective

- Describe new networking and communications functionality being built into Windows 2000
- Positioning of Windows 2000 networking technologies will be discussed

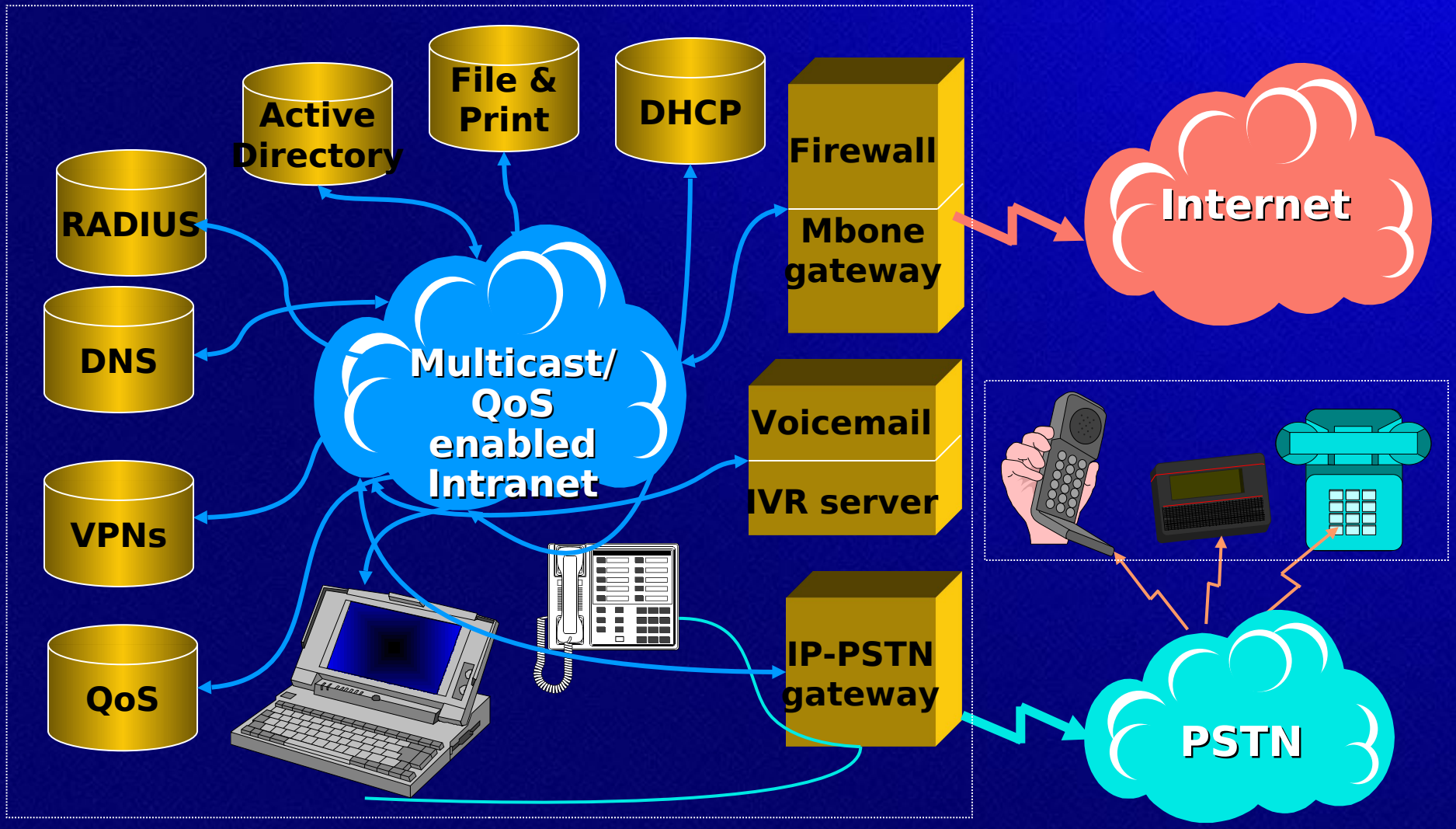
Current State

- The Internet, IP and Web is “IT”
  - Still a lot of IPX and SNA, but…
- More, more, more
  - End systems - PCs
  - Fast systems - CPUs and NICs
  - Bandwidth
  - Users
  - Networked applications - NetShow™, NetMeeting™, etc.
- Advent of the golden age of networking!

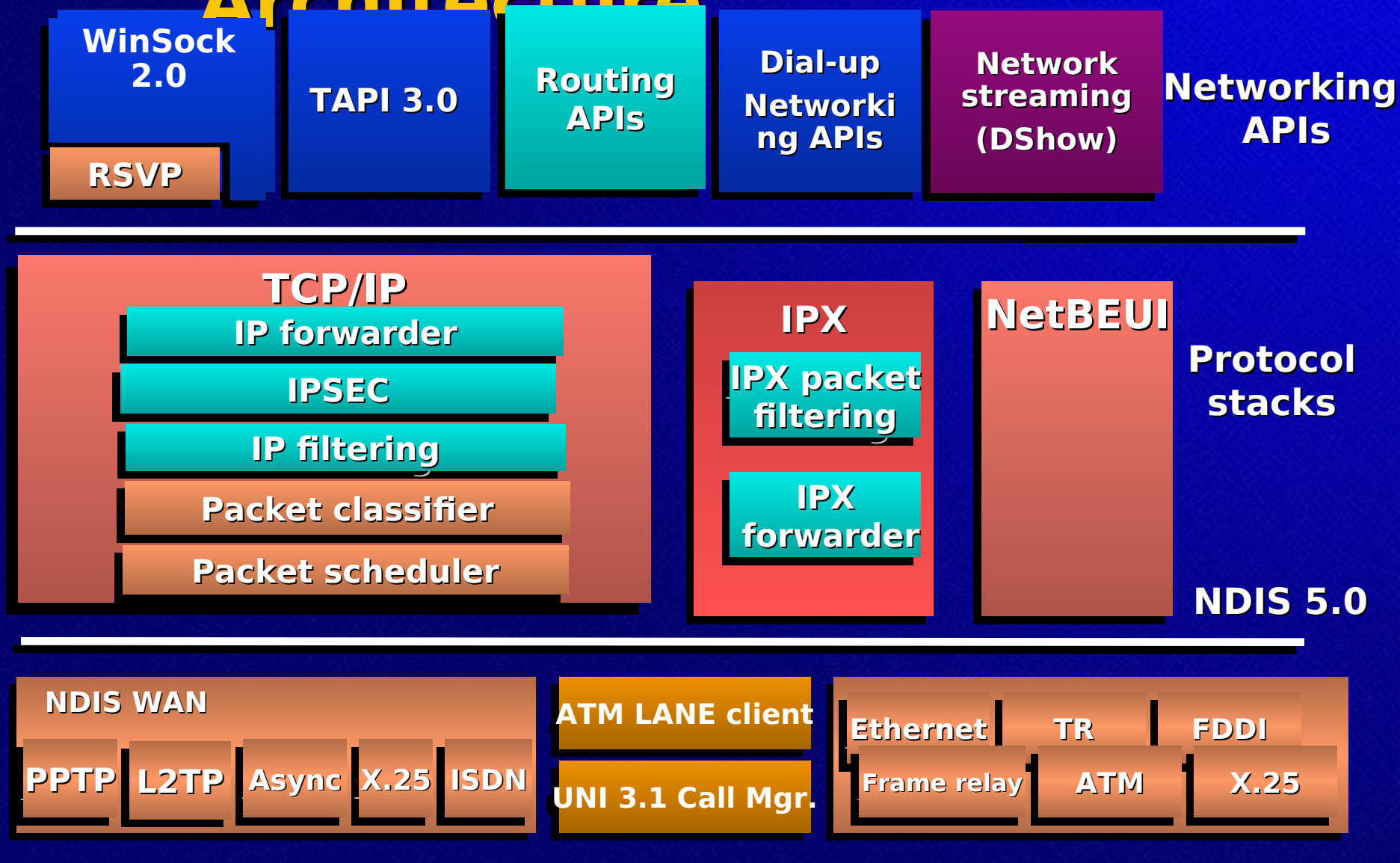
Networking Issues Today

- Too difficult to configure and use
  - TCO for business
  - Barrier to entry for consumers and SOHO
- Complex and inflexible network infrastructure
- Separate voice and data networks
  - High cost - parallel wires, equipment and staff
  - Need scalable and secure communications enhancements for rich content delivery to home, businesses, and public networks
- Security
  - Addressed in networking as well as in the base operating system

Windows 2000 is the Platform For Network Services



Windows 2000 Network Architecture



Windows 2000 Networking

Simpler networking	Easy for end users Easy for administrators Plug and play and power managemen
Programmable network infrastructure	Remote Access Service, Whole sale di Virtual Private Networks Routing Policy Enabled Networking
Communications enhancements	TCP/IP performance and security Network quality of service NDIS for connection oriented media Native ATM support TAPI 3.0 Network as multimedia source/sink

Simpler Networking

Easier end-user networking	▪ TCP/IP installed by default ▪ Automatic addressing for SOHO LANs ▪ Simplified UI for LAN, RAS, and VPN
Easier network administration	▪ MMC tools for RAS, DHCP, DNS, WINS ▪ Improved diagnostics using WMI ▪ Dynamic DNS update by DHCP ▪ Directory for IP security, RAS, QoS
Plug and play power managemen	▪ Windows 2000 for laptops! ▪ Dynamic load/unload of stacks ▪ No power down if network in use ▪ Wake up on directed traffic

Auto Private IP Addresses

- Solution for SOHO LANs
  - Only works for single LAN!
  - Looks for DHCP Server, if no DHCP then do automatic private IP addressing
- Stack picks a private IP address
  - Does conflict detection using DHCP mechanisms
  - Uses NetBIOS naming - broadcast mode
- Will use DHCP Server if a DHCP server comes online
- Windows 98 and Windows 2000

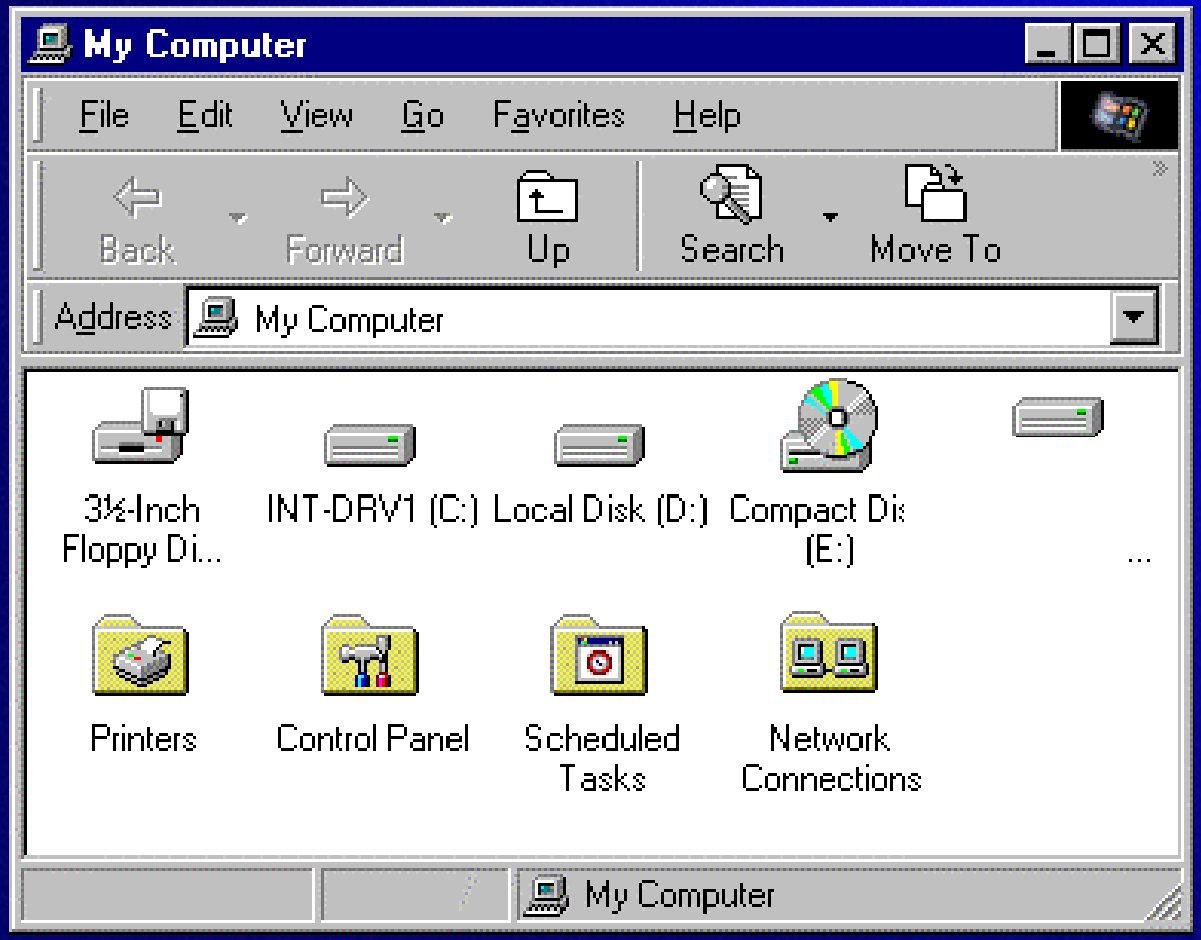
End User UI For Networking

- Network Control Panel is gone
- Connections UI in Windows 2000
  - Unifies config for RAS, LAN, and VPN - “Connection”
  - Look and feel similar to Windows 95 Dial-Up Networking folder
  - Each connection is represented in the folder
  - Can activate and deactivate each connection
  - Properties on a connection for configuration
- Connection Manager for managed dial-up
  - Distributable pre-configured connections
  - Customizable (Connect Actions, Branding)
  - Dynamic phone-book update
  - Dial-up support includes VPNs

Connections UI in Windows 2000

- Simple User Interface for all network connections to/from your machine
- Similar to Win95 DUN connections folder
- Multi-tabbed property sheet defines each connection
- Dial-up and VPN connections very similar
- Represents all LAN and WAN connections
  - Single point of entry for network configuration
  - Simple UI for dial-up and VPN connections
  - Simple UI for NTW server, S/A NTS

Connections UI

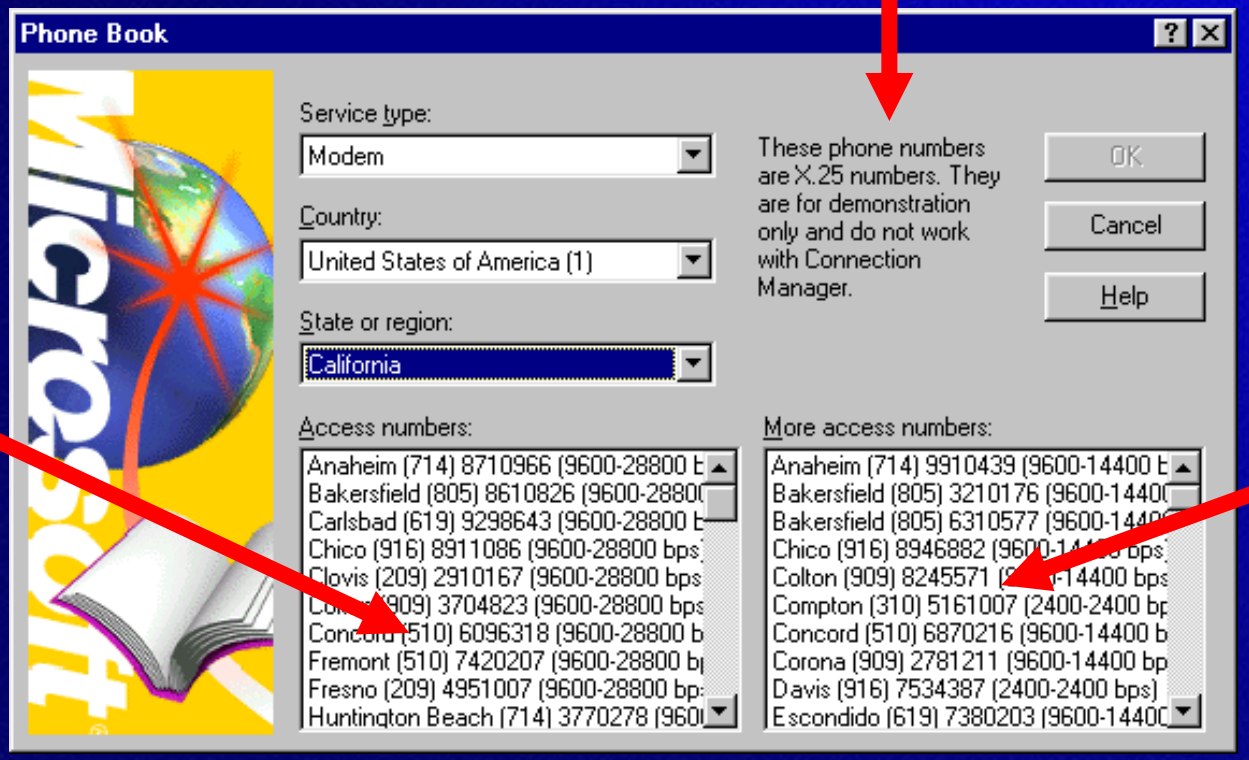


Connection Manager

- Simplifies the Dialing Process
- “Service Profiles” automatically configure client for Internet service
- Validate software installation
- Improve the user experience
  - reliability, user interface, integration
- Extend to support customized Internet Services

Simple and Easy Connections (Dial up and VPN)

Customized message differentiating phone lists



Corporate Phone Numbers which do not require VPN

ISP Phone Numbers which require VPN

Primary Phone-Book **Secondary Phone Books**

Connection Manager will automatically enable/disable PPTP based on the selection of a phone number

Programmable Infrastructure

Remote Access Service	PPP, multi-link, demand-dial, PPTP, 128-bit encryption EAP, RADIUS, BACP, MD5, CM
Virtual Private Networks	PPTP, L2TP, IPSEC Windows 95 and Windows 98 PPTP client
Routing	RIP, OSFP, IPX/RIP, IPX/SAP Multicast forwarding, IGMP proxy, NAT
Manageability	SNMP v1, SNMPv2, WMI MMC snap-ins Policy Enabled Networking

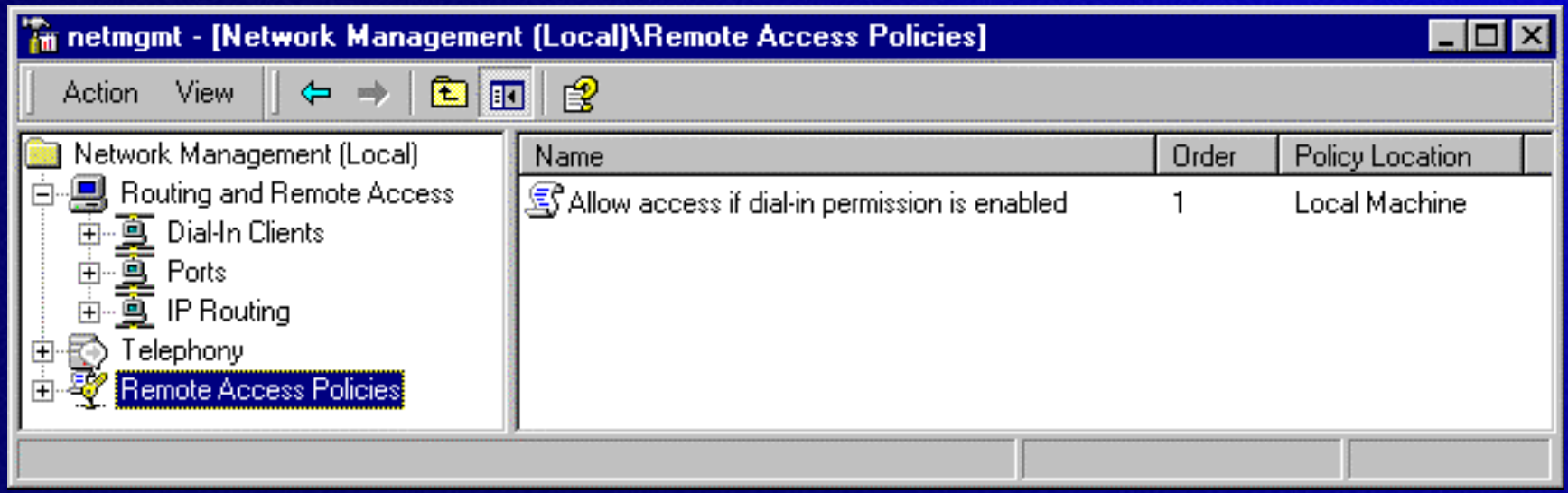
Remote Access Service

- Built in since Windows NT 3.1
  - Multiprotocol: IP, IPX, NetBEUI
  - Compression, Encryption
- Windows NT 4.0 additions
  - Multilink PPP, PPTP
  - Autodial, client, and server APIs
- Windows 2000 additions
  - L2TP, EAP, RADIUS, BACP, MD5, IPSEC
  - Connection Manager (CM)
  - Remote Access Policies

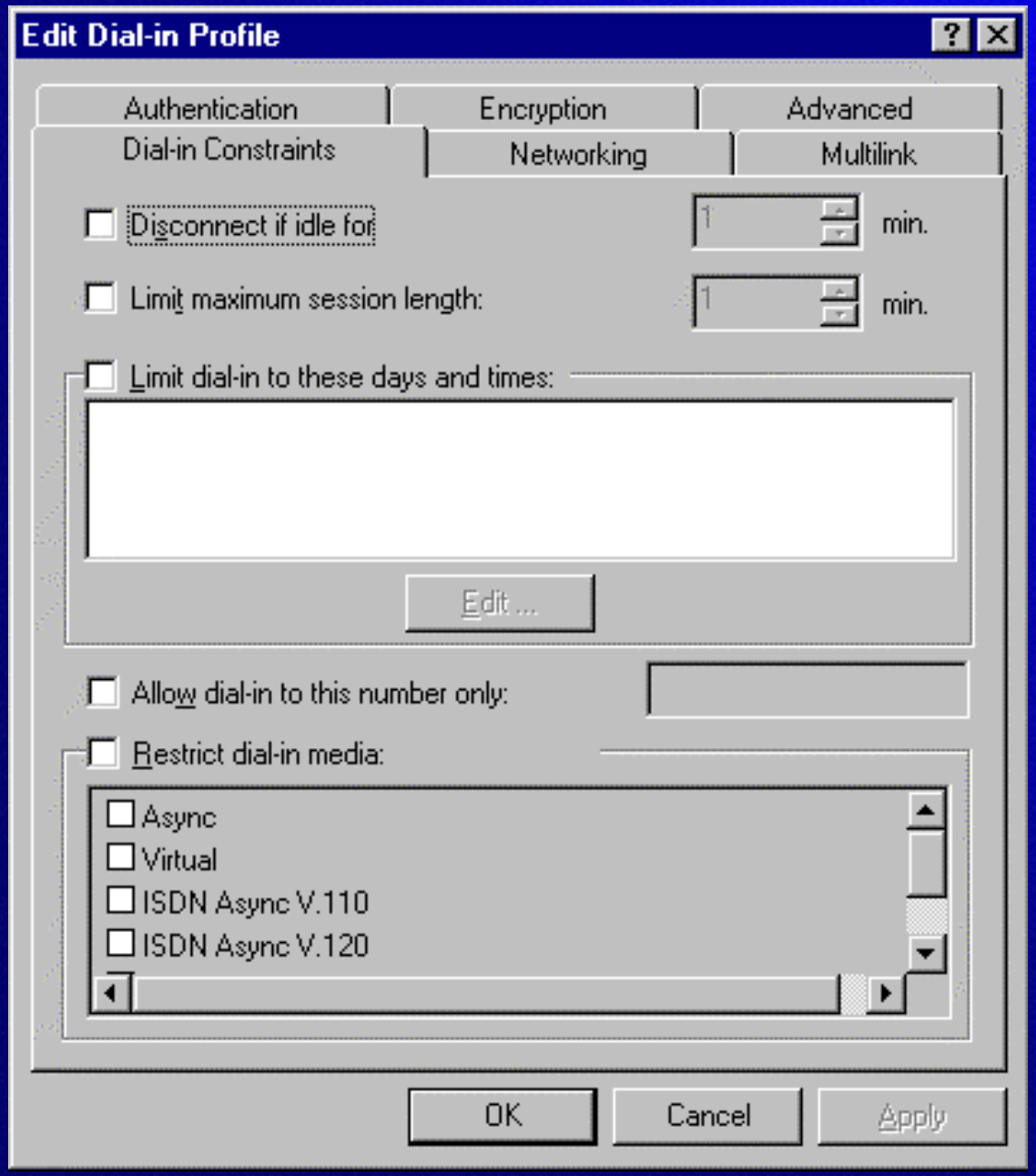
Remote Access Policies

- **Rules-based administration for RAS/VPN**
- **Examples:**
  - **Access by group membership**
  - **Unique rules for VPN access versus dial-in access**
  - **Time of day access restrictions**
  - **Policy = {match rule, access control, profile}**
    - Match rule**: matches on set of connection properties (eg user group, media, time of day..)**
      - Access control**: allow or deny access**
    - Profile**: set of attributes assigned to the connection**
      - **Dial-in constraints (session length, time of day..)**
        - **Authentication requirements (incl EAP)**
          - **Encryption requirements (incl MPPE/IPSec)**
            - **Multilink controls (incl BACP/BAP)**
              - **Network controls (addr policy, IP filters)**

Remote Access Policies



Profile associated with specific policy



VPN Evolution

- 1996: tunneling protocols
  - PPTP (Microsoft, Ascend, 3com, USR) vs L2F(Cisco)
  - Tunneling by network devices
- 1997: standardization and planning
  - L2TP and IPSEC standardization
  - Deployment of tunneling clients
  - Auditing, accounting, and alarming
- 1998: full deployment
  - Centralized user management
  - Network management
  - Enhanced authentication and encryption
- 1999: pervasive VPNs
  - Widespread smart-card adoption
  - Widespread VPN use by telecommuters
  - Seamless integration of VPNs w/ consumer devices

VPN Protocols

PPTP	**Point to Point Tunneling Protocol** Mature technology available for all platforms Windows ‘95, Windows 98, Windows NT 4.0 and 2000 Client-Server, Server-Server
L2TP	**Layer 2 Tunneling Protocol** Internet draft in last call Client-Server, Server-Server - Windows NT 5.0 only
IPSEC	**Internet Protocol Security** Proposed standard Integrated with L2TP in Windows 2000

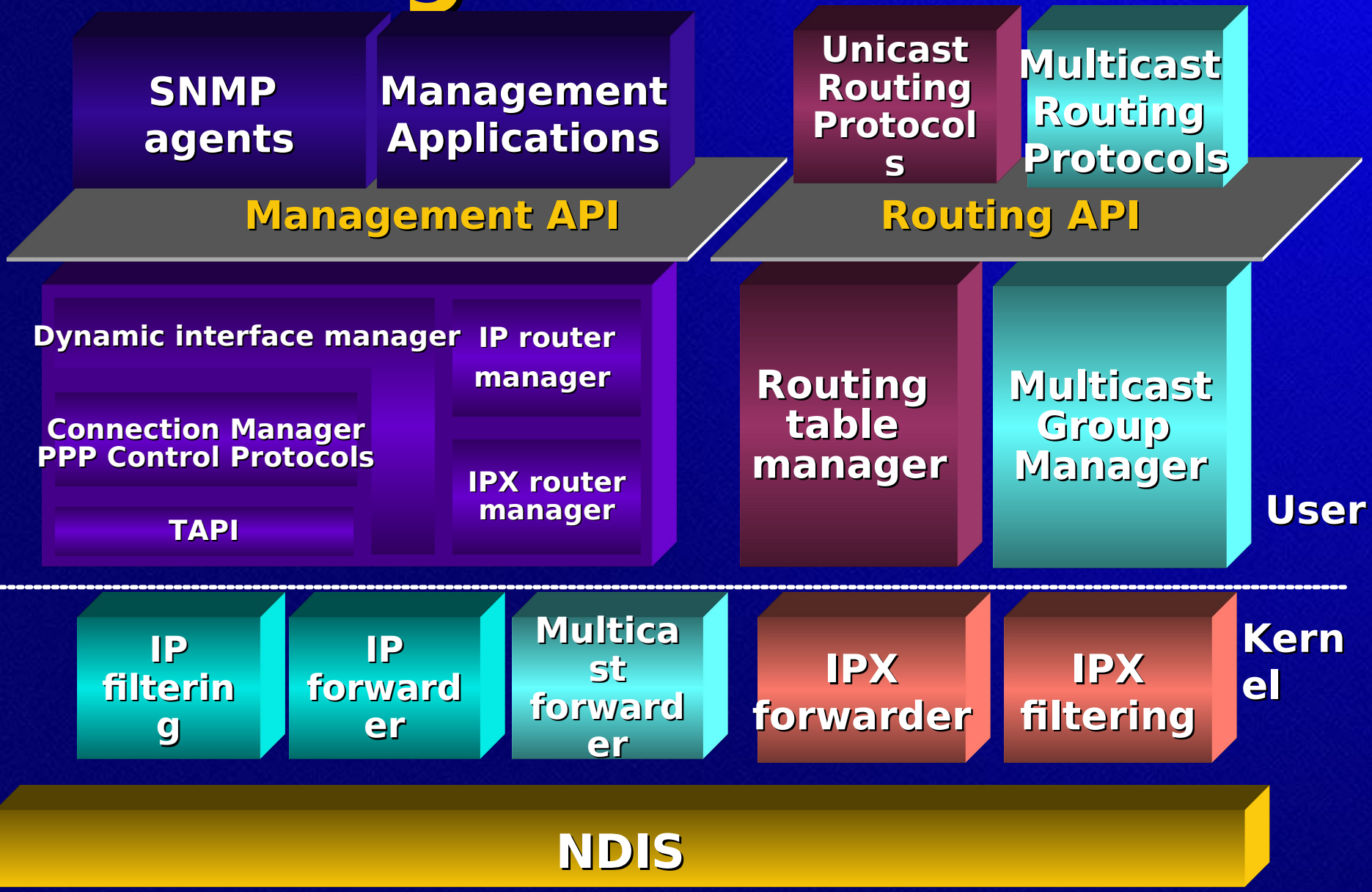
VPN Road Map

- **Tunneling clients and servers**
  - Windows NT 4.0, Windows 2000 - PPTP/L2TP
  - Windows 95 and Windows 98 - PPTP only
- **Multiprotocol support**
  - PPTP and L2TP tunneling protocols
  - Inside tunnels: PPP encapsulation of IP, IPX, NetBEUI, AppleTalk
- **Security**
  - EAP for extensible authentication
  - Built-in public key authentication (EAP-TLS)
  - 128-bit encryption (40-bit outside North America)
  - RADIUS for dial-up authentication, authorization, accounting
  - IPSEC and IKE
- **Management**
  - Connections UI (simpler view of VPN client)
  - Radius client and server
  - Active Directory integration
- **Ease of Use**
  - Connection Manager

Server Integrated Routing

Integrated	Integrated with RAS, VPN, and Active Directory in Windows 2000
Comprehensive	OSPF and multiprotocol RIP NAT Packet filtering Multicast support: IGMP proxy, forwarding
Manageable	Graphical user interface (MMC) Fully remoteable SNMP v2 support Command line interface
Extensible	APIs for Routing, Filtering, Traffic Control Management APIs for customized administration Driver APIs (NDIS)

Routing Architecture



Routing Feature Summary

- Unicast routing protocols
  - IP: RIP, OSPF
  - IPX: RIP/SAP
- Multicast
  - Multicast forwarding
  - IGMP proxy
  - Multicast routing APIs
- RAS and VPN support
  - Demand dial, multilink etc.
  - Routed tunnels using PPTP/L2TP
- Network Address Translation
- APIs for extensibility: Routing protocols, management
- Graphical and command line remote administration interface
- Packet filtering for Performance and security

The Easy to Use Home LAN Solution

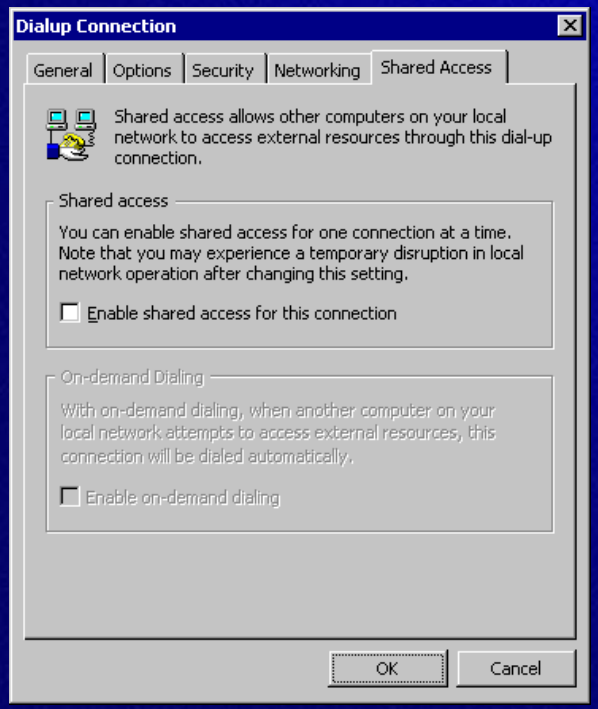
- Simplifies small-scale networking
  - Allows a single Internet connection to be used by multiple machines
  - Sharing a single IP address eliminates the need for manual addressing or DHCP server setup
  - “One click” setup
    - Users need not understand routing to set it up

Connection Sharing Components

- NAT
  - Transparently shares single public IP address for clients on the local-network
  - Translates packets to and from the assigned public IP address
- DHCP allocator
  - Assigns address, gateway and name server on the local-network
- DNS proxy
  - Forwards name-resolution queries
  - Resolves names on behalf of local-network clients
- Auto-dial makes connections automatically
- Transparent VPN access
  - Clients access corporate networks using PPTP through the NAT

Connection Sharing Integration

- Turning on connection sharing for existing connections



Manageability

- New MMC UI
  - Enables creation of custom consoles
- RAS/VPN policy management
  - Profiles for authentication, authorization
  - Conditional profile application: Groups, time of day, etc.
- Policy management for QoS
  - ACS - Admission Control Services
  - Policy per user, per LAN basis
- IP security management using Active Directory
- SNMPv2c
  - WinSNMP support
  - Support for additional MIBs

Communications Enhancements

TCP/IP stack, NDIS 5.0, ATM services, TAPI 3.0

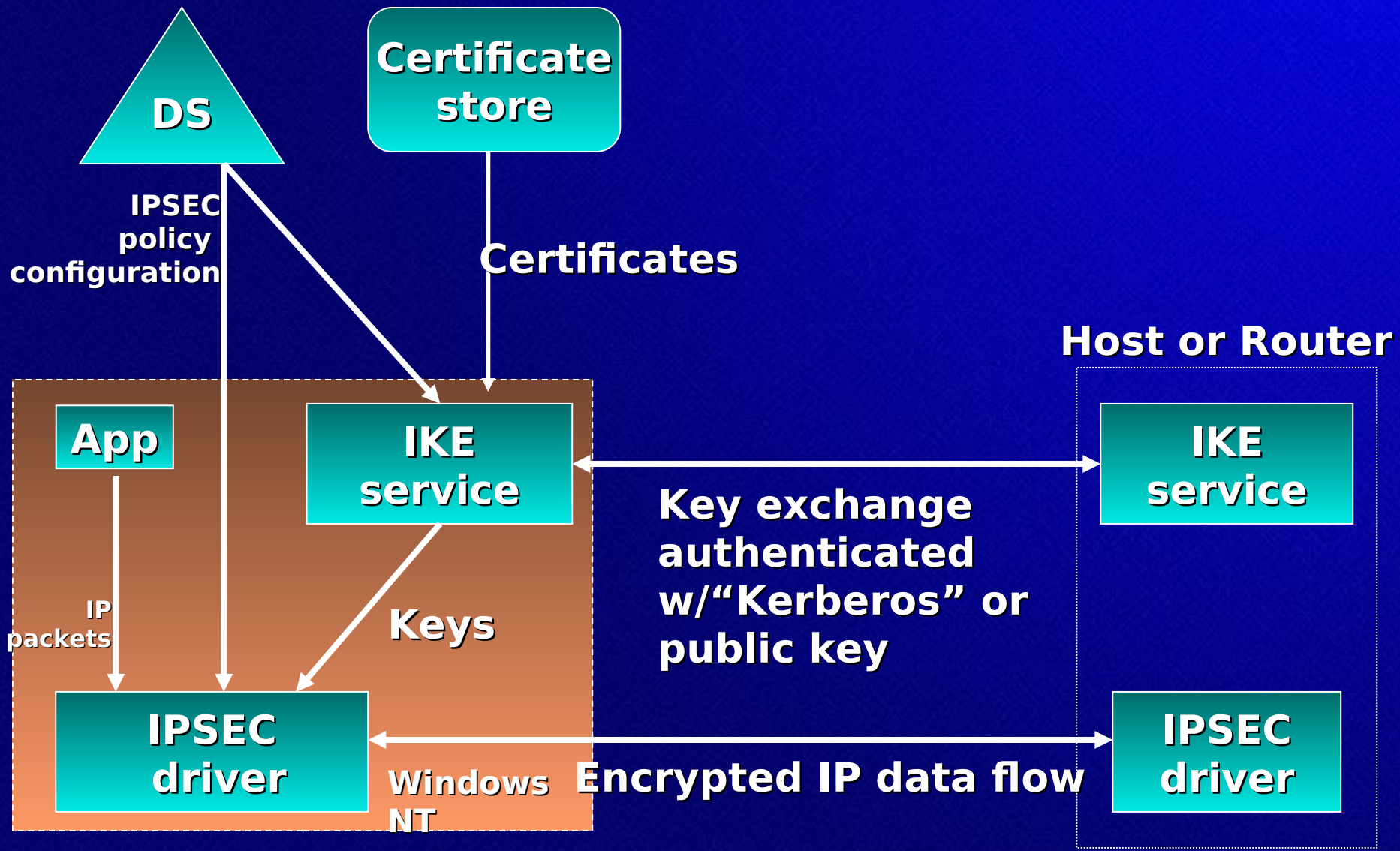
TCP/IP Stack

Performance	▪ Faster stack implementation ▪ Large window support, Selective acknowledgment, ▪ Better roundtrip estimation ▪ Scaled for multi-processors
Security	▪ IP Security with IPSEC and IKE
Quality of service	▪ Winsock 2.0 API ▪ Quality of service (QoS) ▪ Class of service (CoS) ▪ Network resource management

IP Security - IPSEC

- Network layer security using IPSEC
  - End-to-end privacy, integrity, authenticity
- Key management using IKE
  - Internet Key Exchange (IKE)
- Authentication using Kerberos or Public Key Certificates
- Scalable Admin based on Directory
  - Can manage security policy on 1000s of machines using the DS
- Transparency
  - No changes to applications and protocols

IPSEC And IKE



Quality Of Service

- Best effort IP service not good enough for audio/visual real-time traffic
  - Packet loss from congestion, variable delay
- Network managers need to be able to manage their resources
  - Real-time A/V requires bandwidth commitment
  - Mission critical apps need bandwidth protection
- Must interoperate with current infrastructure
  - Ethernet, current generation IPv4, ISP

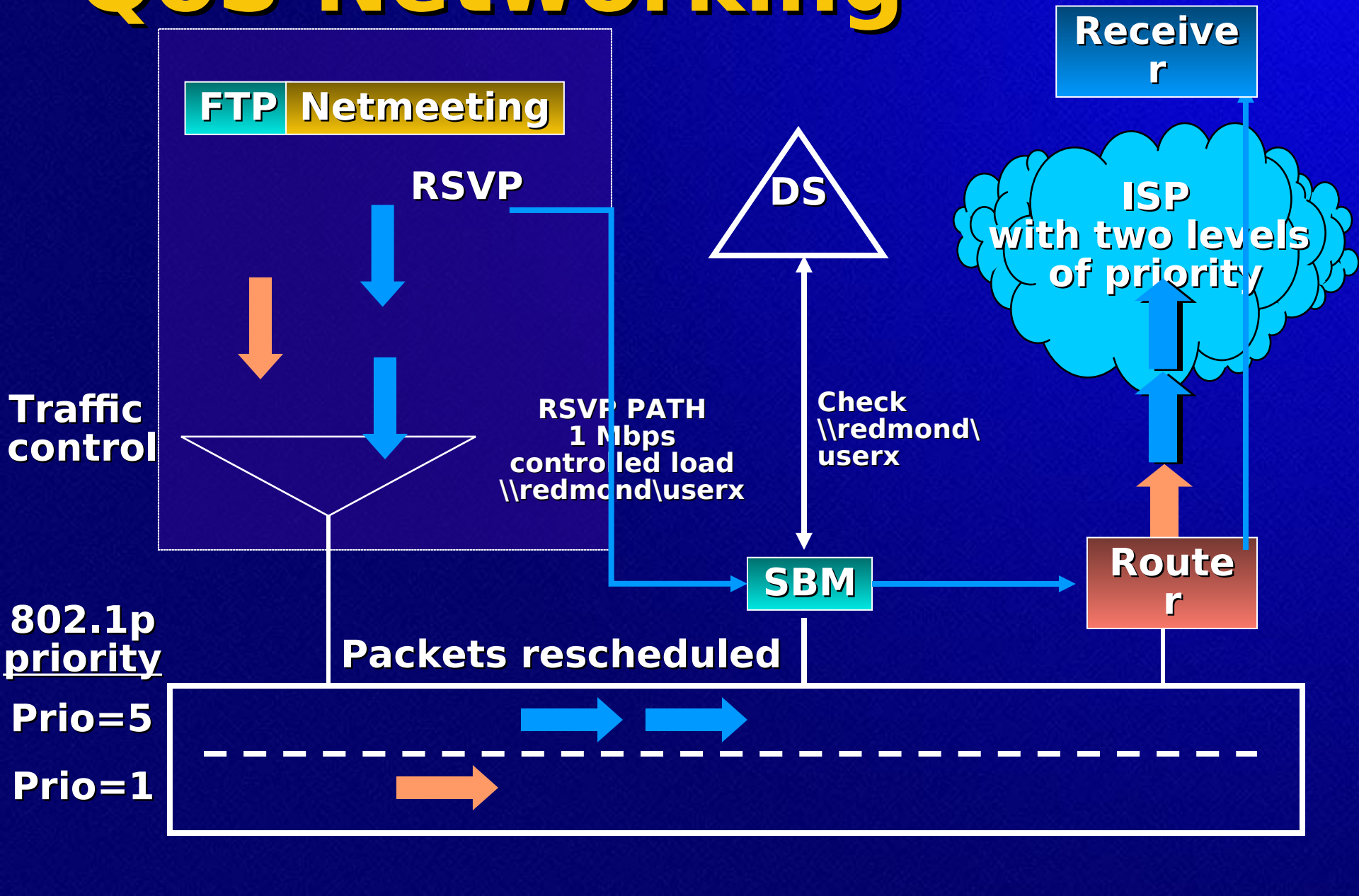
QoS Road Map

	1997	1998-1999
Hosts	No RSVP signaling	RSVP signaling, precedence bits in IP and Ethernet, traffic control
Routers	Low to medium data rate support for RSVP and precedence queuing	RSVP support in border routers, IP switching with precedence queuing
Ethernet switches	High-end switches support 802.1p precedence queuing	802.1p support in most switches and hubs with admission control (SBM)
ISPs	Trial deployments of RSVP	Edge routers map

Windows QoS Program

- New QoS API under WinSock 2.0
- Stack support for QoS
  - Traffic control - queue management in stack
  - Signaling - RSVP, precedence bits in IP header
  - Admission control using ACS
- Shared media admission control service (ACS)
  - Subnet Bandwidth Manager - SBM
  - IETF RSVP effort with Intel, Cisco, 3Com, Extreme, Sun
  - Can control admission into higher priority classes
- Network resource management
  - End system management of traffic control
  - Hop by hop bandwidth management

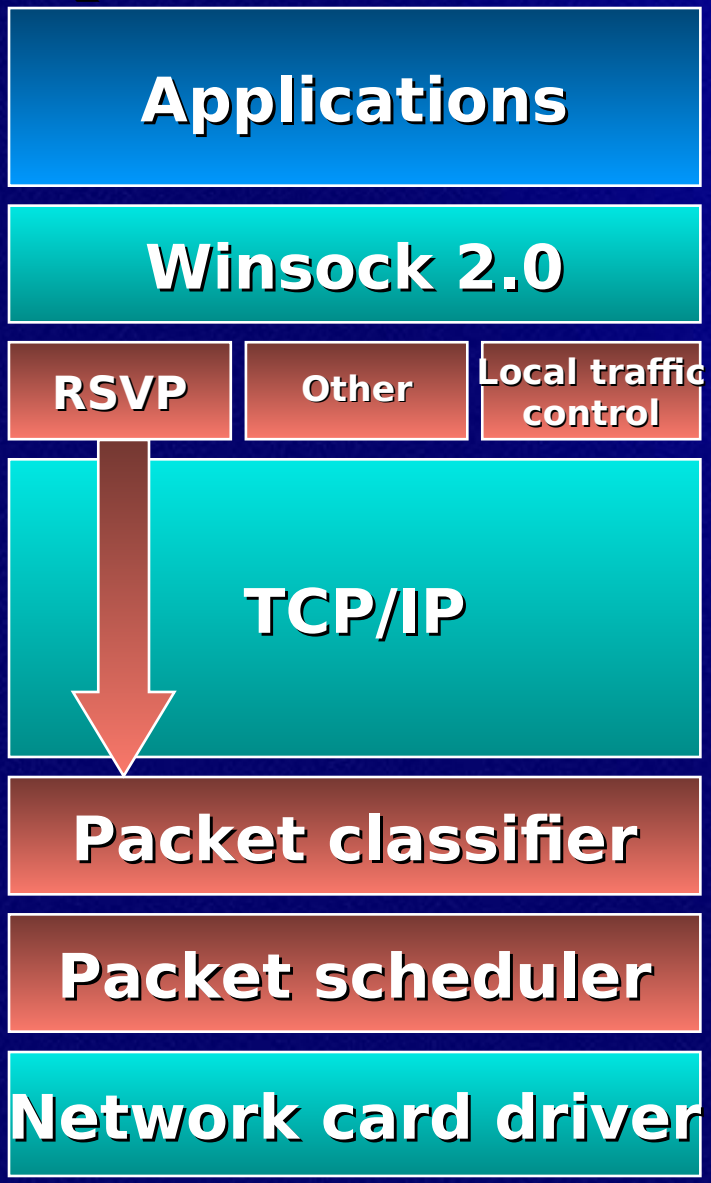
QoS Networking



WinSock 2.0

- New API for networking
  - First released in Windows NT 4.0
- Available:
  - Windows 98 and Windows 2000
  - Release to Web - Windows 95
- Supports
  - Quality of Service - QoS
  - Layered service providers
    - Extension mechanism for networking
    - E.g., remote WinSock for proxy

QoS Architecture



- QoS Service Providers
  - Open and extensible
  - RSVP support built in
- Packet classifier
  - Directs traffic to queues in packet scheduler
- Packet scheduler
  - Delivers queued packets to the network

What About IP Version 6?

- Not in Windows 2000 nor Windows 98
- Microsoft Research has built a prototype
- Product plans for IPv6 in development
- Why do IPv6?
  - Consumer networking
  - Ease of configuration
  - More than 2^{32} PCs!

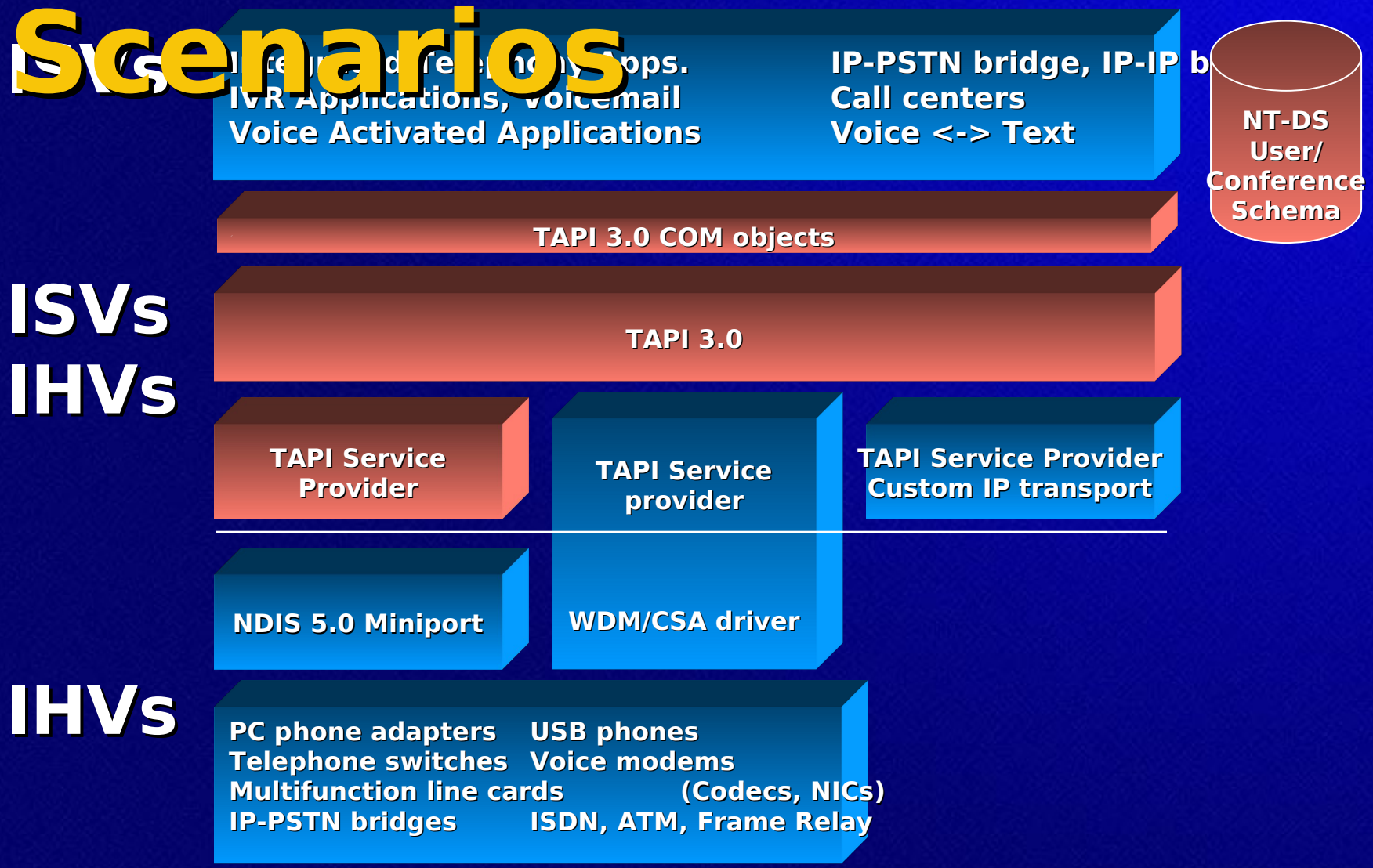
TAPI 3.0

Telephony enhancements to enable multimedia networking for PSTN and IP networks

TAPI 3.0

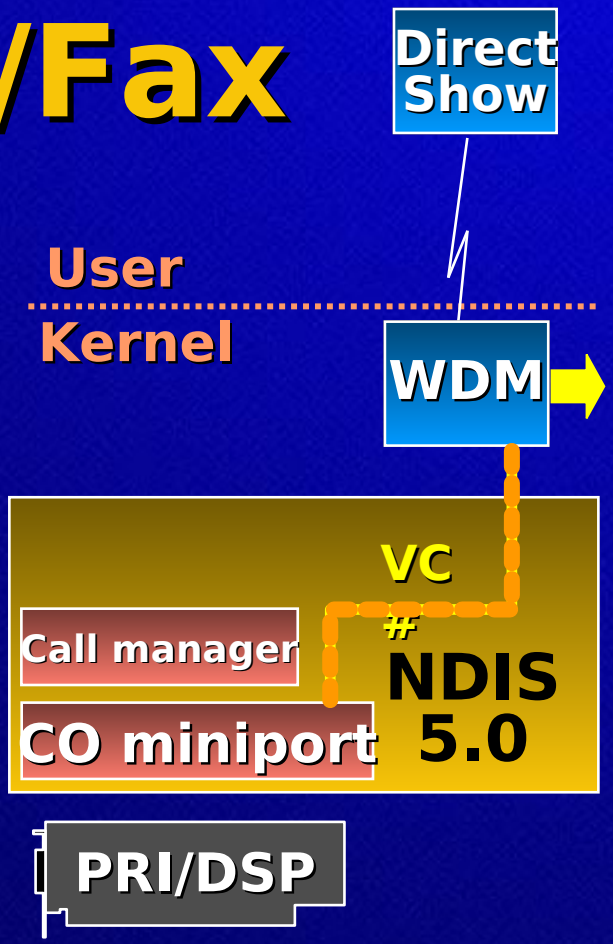
- Unified call control and media streaming
  for PSTN and IP telephony
- Object oriented, language neutral COM API
  - Leverages existing TAPI 2.1 service providers
  - Providers for IP multicast and H.323
- Tight integration with Active Directory
- Enables scalable telephony server

Application Scenarios



Integrated Driver Model For Voice/Data/Fax

- Connection-oriented media
  - ATM, ISDN, Frame Relay ...
- Multimedia source/sink
- WDM streaming integration



Summary

- Key investments
  - Ease of use and manageability
  - APIs and services
  - Networking, telephony, multimedia
- A commitment to standards
  - IETF: L2TP, LDAP, SNMP v2, Kerberos, RADIUS, RSVP, EAP, TLS, IPSEC, TCP/IP
  - ITU: H.323
- Creating the most feature rich and extensible platform for networking
  - Ready for emerging multimedia communications applications and services
  - Ready for virtual private networks and policy-based networking

Action Items

- Enhance the programmable infrastructure
  - Customized and/or extensible management
  - Accounting/Billing
  - New routing protocols
- Telephony
  - Integrate telephony features in new applications
  - Migration to converged voice/data networks
  - QoS aware/enabled applications
- Leverage Windows 2000 for network policy applications for all network devices
- Manageability
  - Services should support WMI, MMC, SNMP